Contract No. NASw - 572

Westinghouse Reference WGD - 38521

RESEARCH ON FAILURE FREE SYSTEMS

Quarterly Report No. 7

Covering the period December 23, 1965 to March 23, 1966

GPO PRICE $ ______

CFSTI PRICE(S) $ ______

Hard copy (HC) 1.00

Microfiche (MF) .50

ff 653 July 65

Prepared for:

The National Aeronautics and Space Administration
Washington, D. C.

Westinghouse Defense and Space Center
Surface Division
P. O. Box 1897 Baltimore 3, Md.

Report Objective and Contract Status Statement

This quarterly report is prepared in accordance with the requirements of contract NASw - 572, between the Westinghouse Electric Corporation and the National Aeronautics and Space Administration. The report describes the work which has been done during the second quarter of the contract extension established by modification No. 5 of this contract. The work to date represents completion of approximately 44% of the extension effort.

MDE 6598

A. BROAD PROGRAM OBJECTIVE

The general objective of this research program is to consider new techniques which are expected to result in significant increases in the reliability of vital electronic systems. These increases will be realized by giving the systems the capability to withstand a large percentage of internal component failures without loss of system functional operation. The scope of this program has included the study of error detecting and error correcting codes, the problems associated with the operation and maintenance of redundant equipment, new schemes for permitting redundant system reorganization in response to changing failure patterns, adaptive logic networks and others.

B. SPECIFIC OBJECTIVES OF THE PRESENT PHASE OF THE PROGRAM

The present phase of this effort has been divided into two distinct sections. The first, smaller portion, provides for the documentation of a computer simulation program which was developed under a previous phase of this contract. The program itself provides a means for performing reliability analyses of a wide variety of failure responsive redundant systems. The objective of the major portion of this phase of the contract is the development of computerized procedures for efficiently allocating a limited number of test points within a redundant system and for estimating the system reliability when one or more components may have failed at the time of estimation.

C. STATUS OF THE COMPUTER PROGRAM DOCUMENTATION

A special technical report, documenting the failure responsive system computer simulation program has been prepared. The report contains a complete description of the program as it is written in FORTRAN IV. Each of the eleven main routines of the program are described in detail, along with input data formats, output options, a list of program variables and constants, detailed flow diagrams of all program routines, and a FORTRAN IV program listing. This report has been completed and is now being reproduced for distribution in April 1966.

D. GENERAL APPROACH TO THE TEST POINT ALLOCATION TASK

To permit the extensive use of redundant digital equipment in spaceborne electronic system implementations, a means must be developed for estimating the probability of mission success based on the results of nonexhaustive system tests. A portion of the previous Failure-Free Systems study was devoted to the development of techniques for systematically distributing a limited number of test points within a redundant system. This study included the development of a technique for properly reflecting information obtained from test points in the estimation of system reliability. To simplify the development of the basic allocation procedure and reliability estimation technique, an idealized system model was used as the vehicle of the study. In the idealized system configuration, statistical independence between stages was assumed. There are two natural extensions of this effort. The first is the expansion of the basic technique to facilitate its use in the analysis of more general, physically realizable systems. The second is the application of the technique to the distribution of test points and the reliability of at least one such system.

To accomplish these extensions, Westinghouse has taken the following approach in a one year development program.

A procedure has been previously developed by Westinghouse, for analyzing the reliability of logically complex order-three, majority-voted redundant digital systems when the condition is given that all components are working at the time of the analysis. The theory of this existing procedure is being modified to provide for the inclusion of the failure state information which can be obtained by making a limited number of subsystem tests. An existing computer program implementation of the procedure will also be appropriately changed to reflect this modification in the analysis procedure. The analysis procedure will then be utilized to produce a test point allocation routine which is capable of optimally distributing a limited number of test points within a broad class of order-three, majority-voted redundant digital systems. Flow charts representing the operation of this procedure will then be prepared.

A computer program will be written to implement the allocation procedure. This program will provide a practical means of applying the allocation procedure to large systems. The computer program implementation of the reliability analysis procedure previously described will become one part of the overall allocation program. The resultant computer program will be documented in enough detail that a design engineer who is unfamiliar with the details of the procedure could be expected to competently use the allocation procedure. One separable part of the documentation will describe the use of the reliability analysis procedure only.

A set of general cost function forms and a supplementary set of rules for establishing cost functions for non-standard stage configurations will be developed. The detailed cost functions for at least one physically realizable system will be established. These cost functions will be inserted into the computerized allocation procedure. The procedure will then be tested by using it to distribute test points to the subsystems of at least one physically realizable system. The one or more systems to which the allocation procedure will be applied will include the Redundant Spacecraft Sequencer previously designed by Westinghouse for the Jet Propulsion Laboratories.

E. ACTIVITY ON THE TEST POINT ALLOCATION TASK

In considering potential modifications to the minimal cuts reliability analysis procedure to reflect test information it has been found that once the system as a whole is known to be working, the expressions describing the probabilities that individual units in a stage are working are no longer statistically independent. Because these probabilities enter into the calculation of unit reliability estimates, these estimates are no longer statistically independent; therefore, any reliability analysis which depends on statistical independence for analytical simplicity cannot be used directly.

Further analysis has shown, however, that if three test points are placed in a stage, then the operational state of a unit is deterministic rather than probabalistic and the unit reliability estimates can again be considered to be independent. This then allows the use of the minimal cuts analysis technique. A similar argument can be used to show that independence can be established for the two test point case. For no test points an alternate solution is available. If R (t) is the reliability of some system as a function of time, then the reliability of the system as a function of time t, $t \geqslant \tau$, given that the system is working at time τ, $\tau \geqslant o$, is given by

$R^1(t) = \frac{R(t)}{R(\tau)}$. Thus the only real problem is for one test point in a stage. Although some preliminary results have indicated that this is never an optimum placement configuration, this problem has not been completely resolved.

The dependence of the present implementation of the minimal cuts analysis on independence of the reliability estimates combined with certain conceptual difficulties associated with this procedure greatly complicates the task of modifying this procedure to fit the present problem. This problem combined with the complications of converting the undocumented FAP language portions of the existing computer program[1] has indicated that an alternative reliability estimation procedure should be considered. The particular procedure which is now being considered as an alternative is one described by D. K. Rubin[2] of J. P. L. The results of a preliminary examination of Rubin's "Block Model Reliability Analysis Procedure" indicate that his procedure would be considerably simpler to modify for the present allocation problem than would be the mininal cuts analysis even though his procedure also relies on independence of the reliability estimates. This advantage is combined with the claim made by Rubin that his procedure produces a greater lower bound (hence, a

[1]Discussed in the previous quarterly report.

[2]Ref: The Placement of Majority Voters within Modularly Redundant Digital Systems

better reliability estimate) than does the mininal cuts analysis procedure and a computational simplicity that implies shorter computing time.

The combined effect of these three advantages and the difficulty of the FAP to Fortran conversion will be sufficient to cause a change to this analysis procedure if the advantages can be verified. The final decision concerning this change will be made on or by April 22, 1966 when the project personnel and Mr. Rubin will confer in Baltimore. Although this will represent a significant change in the technical details of the program no change in schedule or program scope is expected.

The effect of placing test points in a simple, single stage triple redundant system has been analyzed. The value of a particular set of test points is measured by the change in predicted system reliability caused by the information furnished by the test points. Since the amount of information furnished by a test point depends on whether or not the unit(s) tested works, the value of the set of test points is chosen as a weighted average of the change produced in predicted system reliability by the allowable success and failure combinations, or states.

As an example, consider a single stage system with one test point. The unit to which the test point is connected can be either operating or failed; thus, there are two possible system states with respect to the test point. The value of the test point is then:

V = (Probability the tested unit has failed) X | (System "Reliability" given that the tested unit has failed and the system is working at the time of test) - (System "Reliability" (R_N) given only that the system is working at the time of test) | + (Probability that the tested unit is working) X | (System "Reliability" given that both the tested unit and the system are working at the time of test) - R_N |.

The analysis of placing test points in a simple, single stage triple redundant system has been completed. Figure 1 shows a typical set of results. These curves were plotted from successive evaluations of the mathematical expression for the value of test points in a one stage system:

$$V = \sum_{i=1}^{M} P_i \left| R_i - R_N \right|$$

where P_i = The probability of occurrence of the i th state

M = The number of observable states

R_i = The probability that the system will successfully operate until the mission completion time t_m, given that the test points are in state i at test time t_1 and that the system is working at t_1.

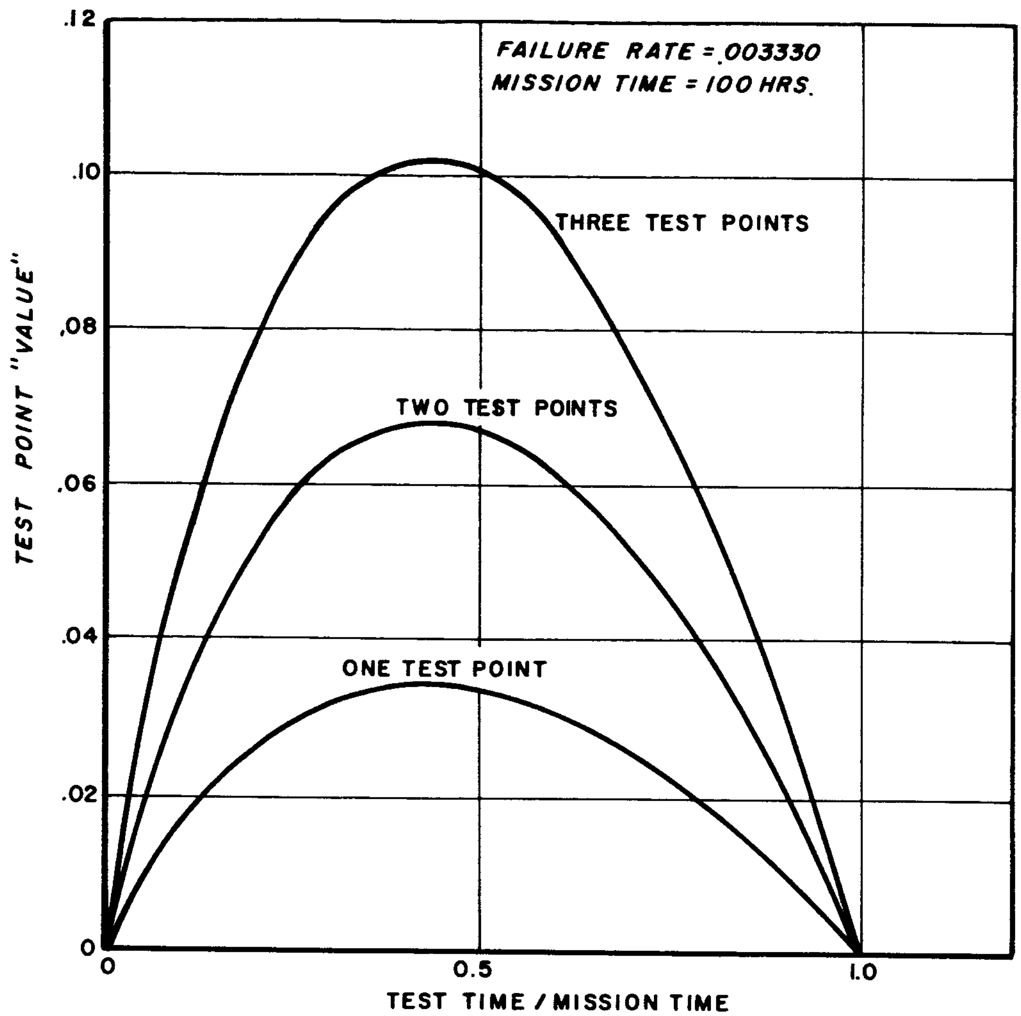

FIGURE 1

R_N = The probability that the system will successfully operate until the mission completion time t_m, given only the information that the system is working at test time t_1. The "values" of test point placement are plotted as a function of test time t_1 and failure rates of the units involved.

As expected, the test points are of no value when the tests are made at the beginning or end of the mission. One result not expected is that each added test point apparently has the same value, regardless of how many test points have been added previously (providing the maximum number is not exceeded). For example, the addition of the third test point has as much added value as the placement of the first test point.

A similar analysis has been performed for two isolated stages (two stages separated by voters) in a system. Preliminary results indicate that for stages of equal reliability with equally costly, perfectly reliable test points, it is of more value to fill up one stage completely than to distribute the same number of points in both stages. Because the cost of each additional test point tends to decrease as a function of the number of test points increases (past one), the above case represents a boundary condition. If this preliminary result can be verified, it will simplify the allocation procedure by drastically reducing the number of feasible test point allocations.

F. TECHNICAL ACTIVITIES PLANNED FOR THE NEXT QUARTER

1. The preliminary result indicating that stages should contain either zero or three test points will be definitely confirmed or disproven.

2. A decision will be made whether to switch to Rubin's Block Model Reliability Analysis Procedure and appropriate computer programming will be begun based on this decision.

3. The development of a generalized value function will be undertaken. The generalized value function is expected to combine features from both the single stage value function described above and the one described on page 2-11 of the final report on phase II of this contract. (This latter value function was developed for the idealized system model described in that report.)

G. MANAGEMENT AND PERSONNEL

The management of this contract continues to be performed by the Advanced Development Subdivision of the Surface Division of the Westinghouse Defense and Space Center. The management personnel with primary responsibility for this program include:

Mr. Sidney E. Lomax, Director of Development
Mr. Theodore Hamburger, Supervisory Engineer

The technical personnel assigned to the program during this contract quarter include:

Mr. Charles G. Masters, Jr., Project Engineer
Mr. Frank B. Cole, Senior Engineer
Mr. Joseph M. Hannigan, Associate Engineer